REMARKS

Claims 1, 2 and 4-19 remain pending in the '852 Application.

Claims 1, 4, 6, 11, 13 and 15 are amended. Limitations of claims 3 are added to claim 1. Claim 3 is cancelled. Claims 4, 6, 11 and 13, which originally depended from claim 3, are amended to depend from claim 1. Claim 15 is amended to clarify language objected to by the Examiner in paragraph 4 of the pending Office Action.

No new matter has been added to the claims by these amendments.

The following remarks attend to all issues presented in the Office Action dated January 09, 2008. Where used herein, numbered subtitles reflect the numbering of issues presented in the aforementioned the Office Action.

4. Claim Objections

Claim 15 is objected to because of the inclusion of "cooperative agent network." Claim 15 is amended to clarify the role of the cooperative agent network in collecting network events for processing by the one or more correlation engines that are also included within the cooperative agent network. The agents and the event correlation engine thus operate together within the cooperative agent network. See for example Figure 4 of the '852 Application and associated description.

5. Claim Rejections – 35 U.S.C. § 103

Given the cancellation of claim 3, claims 1, 4, 6-9 and 15-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,028,338 to Norris et al. (hereinafter, "'338") in view of U.S. Patent No. 7,096,499 to Munson (hereinafter, "'499"). Applicants respectfully traverse.

Initially, Applicants notes that M.P.E.P. §2142 sets forth the criteria that must be met to establish a prima facie case of obviousness: Specifically, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or to combine reference teachings. Secondly, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The following summaries may prove useful in understanding the differences between the '852 Application and the '338 and '499 art.

The '852 Application teaches of installing intelligent, cooperative agents within components of an electronic network, such that the agents cooperate to perform an initial assessment of the network to determine normal activity, monitor the network for abnormal activity and protect the network by blocking abnormal activity, if detected.

On the other hand, '338 discloses a method for providing automatic cooperative response ability to all members of a domain in light of a detected threat or other suspicious activity. A detection server, external to the domain, monitors and parses log and audit records generated by the members. These log and audit records contain information related to the use and attempted use of the member. When the detection server identifies threatening or otherwise suspicious behavior, it sets an alert status in a security profile stored on a profile server. See '338 Abstract. Within '338, agents operate on each member to collect and send the log and audit records for parsing by the detection server. The agents of the '338 method do not evaluate the log and audit information. The log and audit information is related to the use of the member and does not relate to network activity. The '338 Rainforest agents become aware of an alert status by periodically reading the security profile from an external system via a network. The '338 agents do not cooperate to form agents cells, or self organize into agent cells. The '338 agents are configured by Rainforest configuration file. See '338 col. 2, lines 9-15.

'499 discloses an approach to detecting aberrant modes of a software system's behavior based upon behavioral information obtained from a suitably instrumented computer program, as it is executing. The computer program is modified (instrumented) to insert instrumentation points, each of which, during execution of the program, pass control to a mapping module that records activity at that instrumentation point. The mapping module transmits this activity (telemetry) to an execution profile buffer where it is requested from an external program environment. An execution profiler comparator compares the current execution profile with a normal execution profile (previously determined) to identify abnormal software behavior, from which abnormal system behavior may be inferred. See. e.g., Abstract and col. 4, line 53-col. 5, line 5. The '499 approach does not monitor, does not measure, and does not profile, network activity. Thus, the '499 approach is very different from the '852 Application, wherein abnormal activity is determined by monitoring an electronic network through the use of cooperative agent

cells. Monitoring software behavior is not equivalent to monitoring network activity using one or more agents. The '499 approach does not use agents that can be installed into an existing system, but requires that a program within the system be instrumented.

The Examiner's proposed combination of '338 and '499 would require substantial changes to the '338 system. For example, the detection mechanism of '338 is located external to the protected network, whereas for '499, the instrumented program must be located within one of the protected systems. Further, '499 is not agent based and requires instrumentation (i.e., modification) of a computer program within the '338 system. The Examiner makes no disclosure as to where such modification should occur within the '338 disclosed system, nor do the '338 or '499 provide such teaching. The '338 and '499 use different methods that require substantial, non-obvious modification to combine. Section 2143 of the M.P.E.P., states "[i]f the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." M.P.E.P. §2143.01(VI). Accordingly, the rejection should be withdrawn for at least this reason.

Regarding Independent Claim 1: Amended claim 1 recites a method of protecting an electronic network, including:

(a) installing two or more agents within components of the electronic network;

(b) logically connecting the agents into one or more cooperative agent cells;

(c) performing an initial assessment of the electronic network to determine normal activity;

(d) monitoring the electronic network for abnormal activity using the agents; and

(e) protecting the electronic network by blocking the abnormal activity using the agents.

The Applicants concur with the Examiner that '338 fails to teach performing an initial assessment of the electronic network to determine normal activity. The Examiner asserts that it would have been obvious to combine '338 with '499, to render step (c) (previously step (b)) obvious, the motivation being a desire to provide a real time intrusion detection program. However, as noted above, Applicants' interpretation of '338 and '499 suggests that such combination is not obvious, if at all possible, since '338 operates to send logged data to a

detection server for processing to determine suspicious activity, whereas '499 suggests program profiling (i.e., profiling internal performance of a single program) to determine abnormal system behavior. That is, neither '338 nor '499 disclose monitoring an electronic network for abnormal activity using agents. While '338 discloses processing data in an external server, the '499 profiling requires analysis within the system being profiled. The log and activity data collected by agents of the '338 system is not equivalent to, or comparable to, data collected from an instrumented software program of '499. Contrary to the Examiner's assertion, Applicants believe such systems to be fundamentally different in operation and therefore incompatible.

Step (b) of claim 1 recites logically connecting at least one of the agents into one or more cooperative agent cells. Although '338 discloses that each member is provided with a Rainforest Agent, '338 fails to disclose that these Rainforest agents form a cooperative agent cell. The Examiner cites '338 col. 1, line 66 through col. 2, line 15 as rendering this feature (previously in claim 3) obvious. However, although the cited passage discloses grouping of members of a domain, there is no disclosure of cooperation between Rainforest agents or of forming cooperative agent cells, as required by step (b). Within '499, software within a system is modified to allow profiling of the software. However, '499 makes no disclosure of agents, let alone cooperative agent cells, as required by step (b). Accordingly, this feature of claim 1 is missing from the cited art.

Further, '499 is not agent based and therefore cannot operate as an agent installed within an electronic network. More specifically, '499 requires modification of a software program within a computer system to insert instrumentation points, thereby teaching away from the use of agents. Further, '499 teaches a real-time approach to detecting aberrant modes of a software system's behavior. That is, '499 detects aberrant modes of software operation within a computer, and does not monitor a network. The nominal profile for an instrumented program established by '499 is not equivalent to performing an initial assessment of an electronic network.

The Examiner asserts that there would have been motivation to combine '499 with '338 because of the EMERALD program cited in the background of '499. Although Applicants believe that the EMERALD program is similar in operation to '338, neither '338 nor '499 provide any motivation to combine the disclosed operation of '499 with either the EMERALD program or '338. As the Examiner points out, the EMERALD program does not provide real-

time intrusion detection; Applicants concur and also point out that '338 also fails to provide real-time intrusion detection. The '338 agents collect logs and audit records and send them to an external detection server. That is, detection within '338 occurs externally to the protected network. In '499, the instrumented software program generates telemetry information as the software program executes. This telemetry information is first processed by a transducer and then an analysis engine, in which a comparator compares the information to determine if the system activity is nominal or otherwise. Accordingly, there would be no motivation to combine the non real-time detection of the '388 with the '499, which seeks to provide a real time intrusion detection paradigm. Such a combination would counter this stated goal of the '499. See '499 Patent col. 2, lines 3-5.

Applicants would also like to point out that '338 fails to disclose monitoring the electronic network for abnormal behavior using the agents, as required by step (d) of claim 1. As taught by at least paragraph [0020] of the '852 Application, agents form one or more cooperative agent cells to perform monitoring and strategic investigation of suspected activity by mapping agents and attack agents. That is, in step (d) of claim 1, the agents monitor the electronic network for abnormal activity; these agents do not simply collect data for external processing, but also determine abnormal activity. As noted above, the Rainforest agents of '338 simply send log and audit information to the external detection server; these agents do not determine whether activity is abnormal. Further, the log information of '338 that is collected by the Rainforest agents and sent to the log server is disclosed as containing information related to use and attempted use of the members. See '338 col. 5, lines 15-17. There is no disclosure, within '338, of monitoring the electronic network for abnormal activity. That is, the log information of '338 relates to use and/or attempted use of a Rainforest member; there is no disclosure or suggestion that the log information relates to network activity. Applicants also believe that network event information, as monitored by agents of claim 1, could not be transferred to the log server of '338 for processing as the volume of network data would be too much and result in additional network traffic for processing. Accordingly, another feature of independent claim 1 is missing from the proposed '338/'499 combination.

Of note, the information profiled within '499 is based upon execution profiles of software and is not based upon network activity. Thus, even when combined, '338 and '499 do not

perform an initial assessment of the electronic network as required by step (b), nor monitor the electronic network as required by step (c). Thus, two additional features of claim 1 are missing from the cited combination.

For at least these reasons, '338 and '499, even when combined, cannot render claim 1 obvious. Reconsideration of claim 1 is respectfully requested.

Claims 4 and 6-9 depend from claim 1 and benefit from like argument. These claims also have additional features that patentably distinguish over '338 and '499. For example, claim 4 recites that the step of installing further includes: establishing bidirectional communication protocols for agent communication within the cooperative agent cells; delegating one or more agents in the cooperative agent cells to have bidirectional communication with another delegated agent; and establishing bidirectional communication protocols for each delegated agent to communicate with another delegated agent. The Examiner cites '338 col. 5, lines 55-63 as disclosing the features of claim 4. However, '338 fails to disclose bidirectional communication between agents. Broadcasting (described in the cited '338 passage) is not a bidirectional communication. The agents of '338 are not delegated agents that establish bidirectional protocols to communicate with another delegated agent. Also, '338 fails to disclose cooperative agent cells. This shortfall is not overcome by '499. Accordingly, the §103 rejection of claim 4 cannot stand.

Claim 6 recites that the step of logically connecting further includes self-organizing at least one of the agents into each of the cooperative agent cells. As disclosed by '338 col. 2, lines 9-15, Rainforest Agents each have a Rainforest configuration file that tells the Rainforest Agent to which domain the member belongs, to which log server to send log and audit records, and which profile server to periodically query for updates to a security profile. Rainforest Agents are thus organized by the configuration file and are not self-organizing. As argued above, Rainforest agents are not formed into cooperative agent cells. It appears that the cited 'automatic cooperative response ability' of '388 col. 6, lines 10-24 relates to the response of each Rainforest agent to the Alert Status 38 stored in the profile server, and not to the Rainforest agents cooperating as a cell. Accordingly, the §103 rejection fails to establish obviousness of the self-organizing feature of claim 6 within the cited art.

Claim 7 recites that the step of establishing further includes communicating via at least one covert communication protocol. The Examiner cites '338 col. 5, lines 55-63 as disclosing covert communication. However, this cited passage discloses sending a broadcast message via a non-routable protocol, such as NetBios. Broadcast messages over NetBios are far from covert, as required by claim 7. Thus, a *prima facie* case of obviousness is not established

Claim 8 recites that the step of performing an initial assessment includes mapping systems, communication ports and attached devices of the electronic network, and establishing normal activity of the systems, communication ports, and attached devices. Although '499 discloses a calibration mode in which the program is run through as many of the functions and operations performed during a nominal mode, '499 fails to disclose that communication ports and attached devices of the electronic network are mapped to establish normal activity thereof. The "hardware probe" of '499, cited by the Examiner, is understood to be a method of obtaining software module entry and exit points, as commonly known in software profiling. This is not equivalent to mapping systems, communication ports and attached devices of the electronic network as recited by claim 8. For example, the '499 hardware bus is between the processor and memory of one system and therefore is not representative of a network connection. Claim 8 is therefore believed nonobvious in light of the cited art.

Claim 9 recites that the step of monitoring includes (a) non-destructively intercepting communications on the electronic network, (b) collecting events from the intercepted communications and (c) determining if the events indicate abnormal activity. The Examiner cites '338 col. 3, line 63 though col. 4, line 40, as rendering claim 9 obvious. However, '338 makes no disclosure of non-destructively intercepting communications on the electronic network. As noted above, '338 discloses a detection server, external to a protected domain, that monitors and parses log and audit records generated by members of the domain. The detection of '338 is performed external to components of the domain and it would be impractical to route all communication to the detection server of '338 for processing. *Prima facie* obviousness over claim 9 has not been established.

For at least the above reasons, '338 and '499, even when combined, cannot render claims 3, 4 and 6-9 obvious. Reconsideration of claim 3, 4 and 6-9 is respectfully requested.

The Examiner is respectfully reminded that "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply." See MPEP 706.02(j). Applicants request clarification as to the specific items and features of the cited passage that the Examiner construes as rendering claim 15-19 obvious. Applicants were unable to find any of 'correlator,' 'annealing,' 'heuristic' and 'simulated annealing correlator' – anywhere - within '308. Should the Examiner maintain these rejections of claims 15-19, clarification is respectfully requested.

Regarding Independent Claim 15: Amended claim 15 recites a system for monitoring events within an electronic network, including:

(a) a cooperative agent network having two or more agents, each agent installed within one component of the electronic network, the two or more agents forming at least one cooperative agent cell for collecting events from the electronic network, the cooperative agent network further comprising:

(i) one or more event correlation engines, each event correlation engine being connected to the electronic network and having a receive event handler for receiving the events addressed to the event correlation engine; and

(ii) one or more event correlation modules, each of the event correlation modules having an event pattern that defines events of interest, each of the correlation modules receiving all events received by the event correlation engine, the event correlation module correlating the events of interest.

First, as argued above, '338 and '499, alone or in combination, cannot render the cooperative agent network of element (a) obvious, since neither '338 nor '499 disclose or suggest cooperative agents forming at least one cooperative agent cell. Further, neither '338 nor '499 disclose collecting events from the electronic network, as also recited in element (a). Element (i) recites one or more correlation engines each connected to the electronic network. Neither '338 nor '499 disclose a correlation module as recited by element (i). The Examiner cites '338 col. 1, lines 54-67 as teaching elements (a) and (i). However, '338 does not mention correlation – anywhere. Although '499 uses the terms "highly correlated" and "uncorrelated" to describe data, '499 fails to disclose or suggest the action of correlating the data. More

specifically, '499 discloses that "[a] methodology presented herein reduces the dimensionality of the problem from a very large set of program instrumentation points representing small execution domains (modules or execution paths) whose activity is highly correlated to a much smaller set of virtual program domains whose activity is substantially uncorrelated." See '499 col. 4, lines 39-44. That is, within '499, the selected instrumentation points are based upon execution paths that are substantially uncorrelated. Thus, '338 and '499 fail to disclose a correlation engine and event correlation modules and required by elements (i) and (ii).

Alone or in combination, '338 and '499 fail to disclose every feature of claim 15, and therefore '338 and '499 cannot render claim 15 obvious.

Claims 16 and 17 depend from claim 15 and benefit from like argument. However, these claims have additional features that patentably distinguish over '338 and '499. For example, claim 16 recites that the event correlation module is a simulated annealing correlator module. Neither '338 nor '499 discloses an event correlation module nor a simulated annealing correlator module. In fact, neither '338 nor '499 disclose or suggest correlation of data.

Claim 17 additionally depends from claim 16, and benefits from like argument. In addition, claim 17 recites the simulated annealing correlator further includes:

(a) recorded events;

(b) a simulated annealing correlator engine;

(c) heuristics; and

(d) a correlation threshold;

(e) wherein the simulated annealing correlator engine utilizes the heuristics and the correlation threshold to correlate the events received by the event correlation engine with the recorded events, the correlated events being added to the recorded events.

Again the Examiner cites '338 col. 3, line 63 through col. 4 line 10 as rendering claim 17 obvious. However, the Examiner fails to identify each element of claim 17 within the cited passage of '338. The cited passage discloses:

> "The detection server 16 is operable to monitor the log and audit records of the members 20 it is assigned to protect. The detection server 16 parses through these records by applying a threat-detection logic to identify threatening activity. The threat-detection logic may be simple or complex, depending on a number of considerations, including the nature and value of the members 20. For example, in one possible threat-detection logic scheme, suspicious behaviors are associated with threat values, and when the sum of threat values for the domain exceed the Threshold Value 40, a threat is determined to exist. Thus, for example, where three members 20 report suspicious behavior, and the sum of the threat values assigned to these behaviors is "55", and the Threshold Value 40 is "50", then a threat is determined to exist."

In view of the simply stated rejection, Applicants are unable to respond to the cited passage other than to state that the passage fails to disclose recorded events, a simulated annealing correlator engine, heuristics and a correlation threshold. Should the Examiner maintain this rejection, clarification of at least the terms recorded events, a simulated annealing correlator engine, heuristics and a correlation threshold are to be found within the cited passage is respectfully requested. However, even if such clarification is provided, Applicant contends that claims 16 and 17 are both nonobvious over the cited art, both due to their dependence from claim 15, and due to the recitation of a correlation module and simulated annealing correlator in claim 16.

Regarding Independent Claim 18: Claim 18 recites a method of pattern recognition, including:

(a) performing an initial assessment of the electronic network,

(b) collecting electronic network events;

(c) sampling the electronic network events with one or more event correlation engines;

(d) passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine;

(e) comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and, if there is a match, creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution; and

(f) determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution.

The Examiner cites '338 col. 1, lines 54-67 as teaching steps (b) and (c) of claim 18. Respectfully, Applicants disagree. This cited passage recites:

> "The present invention provides a distinct advance in the art of systems, computer programs, and methods of providing computer and network security. More particularly, the present invention concerns a system, computer program, and method of providing an automatic cooperative response ability to substantially all of a plurality of members of a domain in light of a detected threat or other suspicious activity, such as, for example, a virus or denial of service attack.
> In a preferred embodiment, the system broadly comprises one or more instances of a Rainforest Agent; one or more log servers; one or more detection servers; and one or more profile servers. The aforementioned domain is defined as a logical grouping of the members based upon similar risk profiles, determined by such factors or member characteristics as, for example, the members' nature, use, value, and risk tolerance."

Applicants find no disclosure within this passage as to (i) collecting electronic network events as recited by step (b), and to (ii) sampling the electronic network events with one or more event correlation engines as recited by step (c). Further, '338 discloses that "[e]ach member generates log and audit records containing information related to the use and attempted use of the member." See '338 col. 2, lines 7-9. That is, '338 process log and audit records to identify threats to a network and does NOT process network events themselves. Further again, '338 fails to disclose one or more correlation engines for sampling the electronic network events as required by step (c).

The Examiner then cites '338 col. 2, lines 7-24 as showing steps (d), (e) and (f). This cited passage recites:

> "Each member generates log and audit records containing information related to the use and attempted use of the member. Each member is provided with its own separate instance of the Rainforest Agent and a Rainforest configuration file, rainforest.cfg. The Rainforest configuration file tells the Rainforest Agent to which domain the member belongs, to which log server to send log and audit records, and which profile server to periodically query for updates to a security profile.

> The log, detection, and profile servers are dedicated devices protectively located behind a firewall. Thus, security provided by the present invention is administered from a protected position rather than from the exposed members subject to attack. The log server receives and stores in a database all log and audit records generated and sent by the members. The detection server monitors and parses through this stored information using a threat-detection logic in order to identify threatening activity."

Applicants find no disclosure within this passage of: (i) a correlation engine, (ii) correlation modules within each correlation engine, (iii) event matching to an event pattern, (iv) passing of sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine, (v) comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and (vi) creating a new event announcing the match, if there is a match, and (vii) passing the new event to the associated event correlation engine for electronic network distribution, if there is a match.

The Examiner then cites '338 col. 3, line 63 through col. 4 line 10 as disclosing step (f). However, this cited passage (see argument for claim 17, above) fails to disclose (i) a simulated annealing correlator for creating a new event if the pattern is determined to be important, and (ii) passing the new event to the event correlation engine for network distribution.

The Examiner again cites '499 as teaching performing an initial assessment of the electronic network, as recited in step (a). As argued above, '499 does not monitor network activity, and the nominal profile of '499 relates to activity of a software program and not an electronic network.

For at least these reasons, '338 and '499, alone or in combination, cannot render claim 18 obvious. Reconsideration of claim 18 is respectfully requested.

Claim 19 depends from claim 18 and benefits from like argument. However, claim 19 has additional features that patentably distinguish over '338 and '499. Claim 19 recites that the step of sampling further comprises sampling all of, or less than all of, the electronic network events. As argued above, neither '338 nor '499 disclose sampling electronic network events, and therefore cannot disclose or suggest sampling all of, or less than all of, the electronic network events.

Reconsideration of claim 19 is respectfully requested.

Claims 2 and 5 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over '338 in view of '499 and in further view of U.S. Patent Number 7,007,301 to Crosbie et al. (hereinafter, "'301"). Respectfully, Applicants disagree.

Claims 2 and 5 depend from claim 1 and benefit from arguments presented above for claim 1 which are included herein by reference.

Claim 2 recites that the step of installing comprises the step of installing a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents. Claim 5 recites that the step of installing further includes: broadcasting a request for agents to submit to authentication; and authenticating submitted agents.

The Examiner states that the '338 and '499 combination does not explicitly teach a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents. Applicants agree. The Examiner then cites '301, col. 11, lines 1-15, as disclosing agent authentication using SSL communication protocol. However, upon reading and understanding the cited passage of '301, Applicants' believe that SSL provides server authentication and encrypted communication between the agent systems and the management station; that is, SSL allows the agents to authenticate the management station when communicating thereto. As taught by paragraphs [0029] and [0030] of the '852 Application, a type 2 super peer agent authenticates and authorizes active agents such that they may cooperate to form one or more active agent cells. Prior to authentication and authorization, an agent may not join or form a cooperative agent cell. As disclosed in paragraph [0032] of the '852 Application, the type 2 super peer agent may utilize a zero-knowledge authentication protocol to authenticate other agents. See also U.S. Patent Application 10/687,320 for exemplary detail on zero knowledge authentication that may be utilized by the type 2 super peer agent.

The secure connection provided by the SSL protocol and used by '301 is not equivalent to the type 2 super peer agent providing authentication, authorization and reauthorization of agents within the system. SSL provides authentication of a server to a client that allows the client to verify that it is connecting to the correct server. As disclosed by '301, "IDS uses SSL to encrypt all traffic between the management station (i.e., the host running the GUI) and the agent

systems (systems performing intrusion detection)." Col. 11, lines 13-15. The type 2 super peer agent authenticates and authorizes each agent within a system to be protected, such that authenticated and authorized agents may cooperate to form agent cells. That is, within the '852 Application the authentication and authorization is not limited to communication between the agents and the type 2 super peer agent.

The shortfall of '338 and '499 in rendering claim 1 is also not overcome by '301, since '301 fails to disclose performing an initial assessment of the electronic network using the agents to determine normal activity and monitoring the electronic network for abnormal activity using the agents.

For at least these reasons, '308, '499 and '301 cannot render claims 2 and 5 obvious. Reconsideration of claims 2 and 5 is respectfully requested.

Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over '338 in view of '499 in further view of U.S. Patent No. 7,085,936 (hereinafter, "'936"). Applicants respectfully disagree.

Claim 10 depends from claim 1 and recites that the step of protecting comprises one or more of:

(a) luring a malicious agent that causes abnormal activity into a false appearance of success;

(b) planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent;

(c) isolating electronic network components which have been compromised by the malicious agent;

(d) attacking the malicious agent;

(e) formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network;

(f) installing patches to eliminate vulnerabilities in the electronic network;

(g) reassessing the electronic network to detect abnormal operations; and

(h) investigating abnormal operations of the electronic network.

Dependent claim 10 benefits from arguments presented above for base claim 1, included here by reference. For example, neither '338 nor '499 disclose using agents to monitor an electronic network.

The Examiner states that '338 and '499 do not explicitly teach steps (a) and (b) of claim 10. Applicants agree. The Examiner then asserts that '936 teaches steps (c), (d), (e), (f), (g) and (h) of claim 10, since '936 teaches "the system includes a trap system create a virtual cage in col. 7, lines 42-51." Office Action page 10, final paragraph. Respectfully, Applicants disagree.

In summary, the '936 patent discloses systems and methods for detecting intrusions in a host system on a network. A trap host system is located apart from, but connected to, the host system and is configured with a virtual cage into which any detected intruder is diverted. However, '936 fails to disclose cooperative agents for intrusion detection and therefore fails to overcome the shortfall of '338 and '499 in rendering claim 1 obvious.

Step (c) of claim 10 recites isolating electronic network components which have been compromised by the malicious agent. The '936 patent is silent as to isolating compromised components, its modus operandi being to divert the attacker into a trap. Step (d) recites attacking the malicious agent. Again, the '936 patent is silent about attacking the malicious agent, given the use of the trap. Step (e) recites formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network. Again, the '936 patent is silent as to formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network. As disclosed in col. 12, lines 14-18, '936 relies upon a system administrator to block future attacks. Step (f) recites installing patches to eliminate vulnerabilities in the electronic network. Again, '936 relies upon a system administrator to block attacks; '936 does not install patches. Step (g) recites reassessing the electronic network to detect abnormal operations. The '936 patent fails to disclose that the electronic network is reassessed to detect abnormal operations.

For at least these reasons, '338, '499 and '936, alone, or in combination, cannot render claim 10 obvious.

Claims 11-13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over '338 in view if '499 in further view of U.S. Patent No. 7,058,968 to Rowland et al. (hereinafter, "'968"). Applicants respectfully disagree.

In summary, '968 discloses a generic distributed command, control, and communications framework that allows computer systems, devices and operational personnel to interact with the network as a unified entity by allowing local or remote execution of mobile program code, static execution of program code, flexible communication formats, self-healing network techniques, and expansion by the addition of new system modules, software handlers, or mobile autonomous agents. See '968 Abstract.

Claims 11-13 depend from claim 1 (via claim 3) and benefits from arguments presented above for claim 1. These arguments are included herein. For example, neither '338 nor '499 disclose using agents to monitor an electronic network. Further, '968 fails to overcome the shortfall of '338 and '499 to render claim 1 obvious.

Claim 11 recites promoting one of the agents in each of the cooperative agent cells to a cell delegate. The Examiner cites col. 4, lines 44-67 of '968 as teaching that the architecture of the system is design to allow modularity, which allows for the rolls to be reversed. Applicants accept this interpretation of '968, but submit that role reversal within a cell of like agents does not result in promotion of one agent to a cell delegate. First, '968 fails to disclose cooperative agent cells. Second, '968 fails to disclose that one agent within the cooperative agent cell is promoted to a cell delegate. As disclosed within paragraph [0026] of '852, "active agent 34 is promoted to cell delegate 36 if it is the first authenticated and authorized agent of cooperative agent cell 28." The agent promotion of claim 11 is not a role reversal and is not equivalent to the role reversal of '968, since role reversal requires that a cell delegate already exist. Accordingly, a *prima facie* case of obviousness is not established over claim 11.

Claim 12 recites promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent, authenticating new agents with the type 1 super peer agent, and communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity.

Again, the Examiner cites col. 4, lines 44-67 of '968 as teaching that the architecture of the system is designed to allow modularity, which allows for the rolls to be reversed. This argument is deficient on several grounds. First, '968 fails to disclose cooperative agent cells. Second, '968 fails to disclose promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent. As disclosed within paragraph [0027] of '852, "[a]ctive agent 34 and cell delegate 36 may be promoted to T1SPA 38, as necessary, provided that the host component 14 has sufficient resources to support T1SPA 38." The agent promotion of claim 12 is not a role reversal and is not equivalent to the role reversal of '968, since role reversal requires that a type 1 super peer agent already exist. Further, '968 fails to disclose communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity. As argued above, '968 fails to disclose cooperative agent cells and cell delegates. Given these deficiencies, *prima facie* obviousness is not established.

Claim 13 recites that the agents and cooperative agent cells are configured for independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network. In rejecting claim 13, the Examiner again cites col. 4, lines 44-67 of '968 as teaching that the architecture of the system is design to allow modularity, which allows for the rolls to be reversed.

First, Applicants submit that the role reversal of '968 does not disclose independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network. Should this rejection stand, the Examiner's clarification is requested. Second, as argued above, '968 fails to disclose cooperative agent cells.

For at least the above reasons, '388, '499 and '968, alone or in combination, cannot and do not establish a *prima facie* case of obviousness over claims 11, 12 and 13 obvious. Reconsideration of claims 11, 12 and 13 is respectfully requested.

Regarding Independent Claim 14: Claim 14 stands rejected under 35 U.S.C § 103(a) as being unpatentable over '338 in view of '499 in further view of '936. Applicants respectfully disagree.

As noted above, Applicants believe the combination of '338 and '499 to be non-obvious if not impossible, in view of the different operation of each of '338 and '499.

Independent claim 14 recites a system for protecting an electronic network, comprising:

(a) a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate;

(b) a communications protocol within each cooperative agent cell, for (a) communicating between agents of the cooperative agent cell, and (b) communicating with cell delegates external to the cooperative agent cell;

(c) means for determining normal activity levels of the electronic network;

(d) means for detecting malicious activity;

(e) means for isolating compromised components of the electronic network;

(f) means for counter-intelligence to reveal the origin of the malicious activity;

(g) means for repairing damage caused by the malicious activity;

(h) means for determining vulnerabilities in the current protection provided by the plurality of agents; and

(i) means for improving protection to resist future attack on the electronic network.

Element (a) of claim 14 recites a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate. That is, a group of agents form a cooperative agent cell wherein these agents cooperate with one another and promote one agent to be the delegate for the cooperative agent cell. The cell delegate collects and filters data from the other agents within its cooperative agent cell and passes the data to a collection point in the cooperative agent network. See '852 Application paragraph [0026]. The Examiner cites '338 col. 1, lines 54-67 as teaching element (a) of claim 14. However, the Examiner again fails to explicitly identify features of element (a) within the cited passage. The cited passage of '338 fails to disclose any of: cooperative agents, a cooperative agent cell, and a cell delegate. The Rainforest agent of '338 do not cooperate, do not form a cooperative agent cell, and do not represent a cell delegate. See arguments in support of claim 1, above. Applicants believe that each of the Rainforest agents operates independently to send log and

audit records of its member to a designated log server. See '338 col. 2, lines 7-15. The log server is not an agent and is not a cell delegate. Thus, '338 alone does not render element (a) *prima facie* obvious. '499 and '936 likewise fail to teach or suggest this feature, and therefore do not fail to make up for the shortfall of '338 in establishing *prima facie* obviousness of claim 14..

Furthermore, element (b) recites a communications protocol within each cooperative agent cell, for communicating between agents of the cooperative agent cell, and communicating with cell delegates external to the cooperative agent cell. Since '338 fails to disclose cooperating agents, cooperative agent cells, and cell delegates, '338 cannot disclose a protocol for communicating therebetween. Again, the '499 and '936 do not make up for the shortfall of '338, also failing to render element (b) of claim 14 obvious.

Element (c) recites means for determining normal activity levels of the electronic network. That is, the agents monitor network activity during normal operation of the electronic network to determine levels of normal network activity. See paragraph [0020] of the '852 Application. The Examiner admits features of element (c) are not taught by '338. Applicants agree. The Examiner then asserts that '499 teaches "that normal profiles data are initially established by a calibration process that is implemented by running the program in a calibration mode in col. 5, lines 5-15." However, the '499 calibration process is performed for a single running program, and makes no assessment of actual electronic network activity, as recited by element (c). This shortcoming of '338 and '499 is not overcome by adding '936, which also fails to teach or suggest element (c).

Element (d) recites means for detecting malicious activity. As taught by paragraph [0020] of the '852 Application, each cooperative agent cell performs monitoring and strategic investigation of suspect activity by mapping agents 24 and/or attach agents 26. That is, within each cooperative agent cell, agents operate to detect malicious activity by investigating suspect network activity and identifying abnormal activity levels within the electronic network. The Examiner cites '338 col. 3, line 63 through col. 4 line 10 as showing means for detecting malicious activity. However, the detection server 16 of '338 is not an agent cooperating within a cooperative agent cell; the detection server 16 is a dedicated computer system that is external to, but connected to, the networked members. The operation of '338 is different from that of the '852 Application. Again, '499 and '936 fail to make up for this shortcoming of '338, thus, the combination does not provide or suggest element (d) of claim 14.

Element (e) recites means for isolating compromised components of the electronic network. That is, the compromised component is isolated to prevent further malicious activity. The Examiner cites '936 col. 7, lines 42-51 as teaching element (e). Applicants respectively disagree. The trap system 210 of '936 is separate from the protected network and into which an intruder attempting to gain access to the protected system is diverted. This trap system 210 is not a compromised component. For at least this reason, element (e) cannot be rendered obvious by any combination of '338, '499 and '936.

Element (f) recites means for counter-intelligence to reveal the origin of the malicious activity. The Examiner cites '338 col. 4, lines 45-51 as disclosing features of element (f). Applicants respectfully disagree and point out that the cited passage discloses that Rainforest agents broadcast an alert and instruct routers and firewalls to block traffic from particular networks. Counter-intelligence to reveal the origin of the malicious activity is not taught by '338, '499 or '936.

Element (g) recites means for repairing damage caused by the malicious activity. Element (h) recites means for determining vulnerabilities in the current protection provided by the plurality of agents. Element (i) recites means for improving protection to resist future attack on the electronic network. The Examiner cites '936 col. 12, lines 9-29 as teaching features of elements (g), (h) and (i). Although '936 presents information to a system administrator indicating configuration problems that may fit with the factors that made the attack possible, there is no disclosure of a means for repairing the damage caused by the malicious activity as required by element (g), or disclosure of means for improving protection to resist future attack on the electronic network as required by element (i). In particular, '936 appears to rely upon the judgment and action of the system administrator in repairing and improving protection of the network, and thus it is not done automatically within '936.

For at least these reasons, '338, '499 and '936, alone or in combination, cannot render claim 14 obvious. Reconsideration of claim 14 is respectfully requested.

CONCLUSION

In view of the above Amendments and Remarks, Applicants have addressed all issue raised in the Office Action dated January 09, 2008. All pending claims are believed to be allowable. Applicants respectfully request a Notice of Allowance for all of claims 1, 2 and 4-19.

The Examiner is encouraged to telephone Applicant's attorney, Curtis A. Vock, at (720) 931-3011 to discuss the amendments presented herein, or any outstanding issues regarding the '852 Application.

A Petition for Two Months' Extension of Time is filed herewith, extending the period for reply up to and including June 9, 2008. The Commissioner is authorized to charge the $230 extension fee to deposit account No. 12-0600. It is believed that no additional fees are due; however, if any fee is deemed necessary in connection with this Amendment and Response, the Commissioner is authorized to charge the aforementioned deposit account.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 09 June 2008 By: Heather F. Perrin

Heather F. Perrin, Reg. No. 52,884
4845 Pearl East Circle, Suite 300
Boulder, Colorado 80301
Tele: (720) 931-3033
Fax: (720) 931-3001